АКТУАЛЬНІ ДОСЛІДЖЕННЯ МОЛОДИХ НАУКОВЦІВ

UDC 341.231.14:341.33:004.056.5
DOI: https://doi.org/10.31861/jiel.2026.2.56-68

Anastasiia Labyk,
PhD candidate,
Assistant Professor of the Department of International Law and Comparative Law,
Yuriy Fedkovych Chernivtsi National University,
Ukraine
e-mail: a.labyk@chnu.edu.ua
ORCID: https://orcid.org/0009-0005-1376-6771

Mariia Stroich,
Assistant Professor of the Department of International Law and Comparative Law,
Yuriy Fedkovych Chernivtsi National University,
Ukraine
E-mail : m.stroich@chnu.edu.ua
ORCID: https://orcid.org/0000-0003-0328-2851

ON THE ISSUE OF INTERNATIONAL LEGAL GUARANTEES FOR PERSONAL DATA PROTECTION IN THE CONTEXT OF HYBRID WARFARE

This article investigates the complex problem of protecting human personal data during modern armed conflicts, particularly through the prism of hybrid warfare. The rapid pace of digitalization, the advancement of artificial intelligence technologies, and their active integration into the military sphere drive the relevance of this study. These factors cause fundamental changes in the methods and means of warfare, as well as in the very purpose of armed conflict. Today, informational influence and psychological pressure on the enemy's population - which are not always accompanied by a direct armed attack - constitute an integral component of any 21st-century military conflict. Consequently, the study analyzes the concept of hybrid warfare, defining it through characteristic features such as asymmetry, large-scale involvement of non-state actors, latency, and a combination of military and non-military means of struggle.

The research specifically focuses on the role of generative artificial intelligence in the context of growing cyber threats. The paper emphasizes that unauthorized access to individuals' personal data during an armed conflict allows opposing parties to exert targeted psychological influence on population groups or individuals, manipulate public opinion through disinformation and «deepfakes,» and apply illegal filtration and terror against the population.

Furthermore, this study analyzes the current international legal framework regarding personal data protection in conflict conditions. It examines the provisions of international humanitarian law, particularly the Fourth Geneva Convention of 1949. The findings establish that IHL norms lack special provisions for protecting digitized information. Moreover, ongoing discussions among researchers regarding the recognition of digital data as a «civilian object» significantly complicate the qualification of an enemy's actions in cyberspace as a violation of international humanitarian law.

Finally, the article explores the provisions of specific international acts regulating data protection. The analysis determines that the permitted derogation from certain obligations in this sphere can lead to state abuses, often hidden behind the necessity of ensuring national

ISSN 3083-7979

security and defense. Ultimately, the paper highlights that international human rights law, through the provisions of international treaties and the case law of the ECtHR, establishes general guarantees to ensure compliance with the criteria of legality, strict necessity, and proportionality when interfering with the human right to personal data protection.

Keywords: *international law, human rights, artificial intelligence, personal data protection, international legal guarantees of human rights, hybrid warfare.*

Лабик Анастасія, Строїч Марія. До питання міжнародно-правових гарантій захисту персональних даних в умовах гібридної війни.

У статті досліджується комплексна проблема захисту персональних даних людини в умовах сучасних збройних конфліктів, зокрема крізь призму концепції гібридних війн. Актуальність дослідженої теми зумовлена швидкими темпами цифровізації, удосконаленням технологій штучного інтелекту та активним впровадженням їх у військову сферу, що зумовлює докорінні зміни у методах та засобах ведення воєнних дій, а також власне меті збройного конфлікту. На сьогодні інформаційний вплив та психологічний тиск на населення ворожої сторони, які не завжди супроводжуються безпосереднім збройним нападом, набувають статусу невід'ємної складової будь-якого військового конфлікту XXI століття. У ході дослідження проаналізовано концепцію гібридної війни, яка розкривається через сукупність таких характерних рис як асиметричність, масштабне залучення недержавних суб'єктів, латентність, поєднання засобів військової і невійськової боротьби та інших.

Особливу увагу приділено ролі генеративного штучного інтелекту в контексті зростання кіберзагроз. Зосереджено увагу на тому, що несанкціонований доступ до персональних даних осіб у ході збройного конфлікту дозволяє його сторонам здійснювати точковий психологічний вплив на групи населення чи окремих осіб, маніпулювати суспільною думкою через поширення дезінформації та «дипфейків», а також застосовувати незаконну фільтрацію та терор щодо населення.

Здійснено аналіз чинної міжнародно-правової бази щодо охорони персональних даних в умовах конфлікту. Досліджено положення міжнародного гуманітарного права, зокрема положення IV Женевської конвенції 1949 року. Встановлено, що норми МГП не містять спеціальних положень для захисту оцифрованої інформації, а серед дослідників досі тривають дискусії щодо визнання цифрових даних «цивільним об'єктом», що значно ускладнює кваліфікацію дій ворога у кіберпросторі як порушення міжнародного гуманітарного права.

Досліджено положення спеціальних міжнародних актів, які регулюють питання захисту даних. Визначено, що передбачена ними можливість відступу від окремих зобов'язань у даній сфері може призводити до зловживань держав, прихованих за необхідністю забезпечення національної безпеки та оборони. Зазначено, що міжнародне право прав людини через положення міжнародних актів та прецедентну практику ЄСПЛ встановлює загальні гарантії щодо дотримання критеріїв законності, суворої необхідності та пропорційності при втручанні у право людини на захист персональних даних.

Ключові слова: *міжнародне право, права людини, штучний інтелект, захист персональних даних, міжнародно-правові гарантії прав людини, гібридна війна.*

Introduction. The advancement of the digital realm and artificial intelligence technologies has confronted the modern world with unprecedented challenges in

ISSN 3083-7979

safeguarding human rights. Consequently, the international community must regulate human activity in the virtual environment using novel legal instruments and methods. Traditional mechanisms, despite their proven efficacy in physical space, often prove entirely ineffective in cyberspace. A prime example of this regulatory transformation is the shift away from the prevailing model of retrospective rights protection. Under this traditional approach, rights are protected post factum - after a violation or restriction has occurred — through restitution or compensation for damages. However, given the unprecedented speed of data exchange and information dissemination in the digital environment, this retrospective model is gradually losing its efficacy. The scale of damage resulting from conventional offenses is often incomparably smaller than the harm caused by cybercrimes. This necessitates the adoption of preventive regulatory frameworks for digital rights, an approach the European Union is currently actively implementing [19, p. 219].

The concept of preventive protection acquires paramount importance in the context of contemporary hybrid warfare, where digital technologies transform from conventional communication means into veritable weapons of war. Personal data proves particularly vulnerable in this environment, frequently serving as an instrument through which states or military formations attempt to exert extensive influence over geopolitical processes. For instance, P. Perez-Sales identifies three levels of interference with the right to privacy, executed through the processing of vast datasets of personal information: a) psychological impact, which entails collecting and processing data on an individual's psychological state and their attitudes toward specific processes or phenomena. This information can subsequently be weaponized to influence specific population groups, foster prejudice, identify vulnerabilities, extract intelligence, manipulate decision-making, and undermine resistance; b) social control, exercised through the analysis of personal data to categorize populations. Streamlining the identification and division of society into groups based on specific traits provides extensive capabilities for tracking, isolating, selectively coercing, and controlling individuals; c) social impact, which shares many characteristics with psychological impact but is distinguished by its scale and broad scope. In this scenario, the target (or rather, the victim) of such interference is rarely a single individual, but typically a social group or society as a whole. In the context of armed conflict, these levels manifest through disinformation, intimidation, and manipulation, as well as the deployment of lethal autonomous weapons systems and the coordination of both cyber and kinetic attacks against civilian infrastructure [11, p. 5-6].

Certain states have long expressed concerns regarding the security of personal data processed by private corporations. A relatively recent example is the 2025 ban on the TikTok mobile application in the United States, which resulted in the complete restriction of access for registered users within 24 hours and suspended new registrations for the subsequent three weeks. This decision was publicly justified on the grounds of US national security interests, citing the alleged ties between the platform's owners and the political leadership of the People's Republic of China. Although most of the information regarding the legal challenge to the prohibition act remained classified, numerous analysts suggest that TikTok's privacy policy concerning the collection and processing of user data served as the most probable grounds for the restriction. Additionally, some researchers emphasize the risks of Chinese narratives influencing public opinion on the most sensitive issues within American society [7, p. 2]. Despite the subsequent reinstatement of the platform in the United States, this case starkly illustrates the challenges confronting the international community.

An analysis of the contemporary international legal framework for personal data

ISSN 3083-7979

protection, particularly within the context of hybrid armed conflicts, reveals the inadequacy of existing regulatory guarantees, which remain focused on traditional means and methods of warfare. Current legal norms prove insufficient to safeguard the personal information of individuals participating in armed conflicts or residing in active combat zones. In light of these challenges, this study analyzes the existing international legal framework for personal data protection during wartime to identify regulatory gaps and formulate recommendations for enhancing both universal and regional guarantees to secure personal data in the era of hybrid warfare.

The objective of the article is to examine the current state of international legal regulation regarding personal data protection in the context of contemporary hybrid warfare.

Literature Review. The issues of hybrid warfare, the application of emerging technologies in armed conflicts, and the protection of human rights in the digital environment remain the focus of numerous domestic and international scholars. Specifically, military theorists such as F. Hoffman, M. Galeotti, E. Luttwak, L. Freedman, T. Rieder, A. Kyrychenko, S. Ivanenko, V. Remez, V. Aleshchenko, O. Baranovskyi, T. Andriievskyi, V. Holovchenko, and Yu. Uzdienova have extensively analyzed the conceptual foundations of hybrid warfare, its evolution, asymmetry, and the blurring boundaries between military and non-military means of engagement. Furthermore, the works of P. Perez-Sales, B. Shiner, S. A. Teo, A. Ünver, T. Roberts, and M. Oosterom address the issues of informational and psychological influence on civilian populations, as well as the instrumentalization of personal data. Despite this substantial body of literature, most studies primarily focus either on the general aspects of cyber warfare and critical infrastructure protection or on personal data protection during peacetime. However, the international legal status of personal data specifically as a distinct instrument of manipulation, control, and terror in the context of modern hybrid warfare remains insufficiently explored.

Results and Discussion. To ensure a comprehensive and objective analysis of the international legal framework governing personal data protection during armed conflicts, it is first necessary to define the concept of «hybrid warfare» Originating in the United States in the early 2000s, this term has undergone significant conceptual transformations and refinements. Frank Hoffman, one of the pioneers of this framework, identified the reassessment of conflict objectives as a critical distinguishing feature of modern hybrid warfare. Specifically, he noted that in the 21st century, the strategic focus has shifted away from territorial conquest toward destabilizing the adversary and sowing chaos within its borders [17, p. 87]. The researcher traced the evolution of this concept through categories such as «fourth-generation warfare,» «compound warfare,» «unrestricted warfare,» and «multi-dimensional warfare,» demonstrating the deep historical roots of the hybrid warfare framework. Notably, each of these conflict types exhibited an increasing number of features that distinguished them from traditional wars. For example, the author characterizes fourth-generation warfare by the blurring of lines between lawful combatants and non-combatants, as well as the significant influence of non-state actors on the conflict's trajectory. In contrast, the concept of «unrestricted warfare,» introduced by Chinese military strategists, illustrates the impact of globalization on modern armed conflicts by expanding their scale, weaponizing new domains, and deploying emerging technologies [9, p. 18-27].

Furthermore, justifying the application of the term «hybrid» specifically to 21st-century armed conflicts, F. Hoffman illustrates their defining features using the 2006 Hezbollah campaign as a case study. The nature of these operations manifested through: a)

ISSN 3083-7979

the integration of a well-organized political movement with guerrilla warfare tactics; b) combat asymmetry, characterized by the strategic exploitation of urban terrain, the imposition of close-quarter engagements, high force dispersion, and the execution of operations in extreme proximity to civilian populations or non-combatants; c) the active deployment of heavy weaponry, including anti-ship and anti-tank missile systems - capabilities traditionally uncharacteristic of non-state actors; d) electronic intelligence and the deployment of armed unmanned aerial vehicles; e) large-scale information campaigns and media dominance [9, p. 35-38]. Thus, the 2006 Second Lebanon War marked the dawn of a new era in military confrontations and the genesis of the hybrid warfare concept, which continues to undergo active development today.

By analyzing Hezbollah's military strategy at the time, the Russo-Georgian War, the Syrian Civil War, the armed conflicts in Iraq and the Gaza Strip, and numerous other conflicts that have erupted or persist since the early 21st century, researchers have identified distinct characteristics defining hybrid warfare. The primary distinguishing feature is the blurring of boundaries between peace and war; even in the absence of active kinetic hostilities, adversaries employ instruments of informational influence, economic coercion, and cyberattacks. A second critical characteristic is its frequently latent nature, manifested through a state's denial of involvement in a specific conflict or its very existence, coupled with the obfuscation of strategic objectives. Another defining feature is complexity, achieved by integrating an adversary's active operations across three concurrent levels: 1) directly along the front line involving regular armed forces; 2) behind enemy lines through guerrilla or insurgent movements, as well as terrorist activities; and 3) in the international arena utilizing non-military instruments. Directly linked to this complexity is the inherent asymmetry of hybrid wars, where establishing a clear front line becomes impossible as the conflict extends far beyond a state's land, maritime, and airspace territories, increasingly transcending physical space entirely. Regarding the role of non-state actors, unlike traditional conflicts, hybrid warfare actively leverages private entities such as terrorist organizations, private military companies, hacker groups, corporate representatives, and non-governmental organizations. Notably, attacks are often comprehensive and sudden, simultaneously deploying geographically dispersed military and non-military instruments to destabilize the adversary rapidly and inflict irreparable damage. Furthermore, an indispensable feature of modern hybrid warfare is the dominance of cognitive influence: today, ideological, informational, and psychological warfare are gaining unprecedented importance, gradually displacing traditional means and methods of combat. Finally, researchers emphasize that 21st-century conflicts are characterized by a pervasive disregard for international treaties and customary norms governing the laws of armed conflict [17, p. 87].

Considering these characteristics collectively, it is difficult to dispute that integrating military and non-military elements creates substantial obstacles to the identification and peaceful resolution of hybrid conflicts. Furthermore, analyzing the concept of hybrid warfare through the lens of the past two decades reveals that, despite the immutability of its core essence, the methods and means of warfare have undergone significant transformations. Scholars note that the onset of Russia's full-scale invasion of Ukraine has unveiled new dimensions of this concept. The emergence of these novel aspects stems not only from shifting paradigms in warfare but also from the rapid pace of digitalization in recent years, particularly - though not exclusively - the advancement of artificial intelligence technologies [17, p. 91].

Generative artificial intelligence has emerged as a profound contemporary

ISSN 3083-7979

breakthrough, offering humanity unprecedented opportunities to enhance and automate numerous industrial processes, streamline information retrieval, and generate digital content. These technologies have also permeated the military domain. Currently, developers are actively leveraging AI to design advanced air defense systems, robotic platforms, and autonomous combat drones. These innovations aim to minimize direct human involvement in combat operations, thereby reducing military personnel casualties through precision strikes against military targets [15, p. 6]. Furthermore, artificial intelligence has become an indispensable instrument of information warfare, the scale of which now spans nearly the entire globe. By generating vast arrays of images, videos, audio files, documents, messages, and alerts, AI has precipitated a novel form of information asymmetry in modern hybrid warfare, whereby the volume of data vastly outpaces the human capacity for critical evaluation. Under the chronic stress of armed conflict, an individual's cognitive ability to analyze incoming information deteriorates significantly, rendering them highly susceptible to narratives propagated by the aggressor state. The latter, in turn, exploits disinformation and deepfakes to exert psychological influence over the civilian population, cultivating emotions such as grief, sympathy, fear, or perceived responsibility for the actions of political leadership. Crucially, the ability to execute these psychological operations in a highly targeted manner significantly amplifies their overall effectiveness [16, p. 57].

Deploying targeted cognitive influence over individuals requires access to their personal data, which enables the identification of demographic categories most vulnerable to specific forms of manipulation. The construction of optimal influence strategies depends on acquiring information regarding a specific individual's social connections, lifestyle, health status, location, beliefs, and preferences. Practical evidence demonstrates that belligerent parties may actively collect and process personal data to ascertain political affiliations, identify individuals loyal to the opposing side, and terrorize civilian populations in occupied territories. A stark example of such conduct is the actions of the aggressor state's representatives in the territories that fell under the control of Russian armed forces following the full-scale invasion. Specifically, human rights monitors documented the mass collection of mobile device identification numbers, passport numbers, tax identification codes, biometric data, images, contact lists, and numerous other data types. Russian intelligence services weaponized this information to identify individuals who had participated in combat operations, belonged to Ukrainian military formations, or were affiliated with such personnel [6].

In contemporary conditions, where digitalization encompasses nearly every sphere of human activity, personal data is continuously introduced into the digital environment through state and municipal registries, diverse web resources, social networks, and applications. Consequently, an urgent necessity arises to protect these data from escalating cyber threats. It is undeniable that hacker attacks, functioning as elements of hybrid warfare, threaten not only the life, health, and right to privacy of individuals, but also possess the capacity to inflict irreparable damage upon national and public security, thereby undermining state defense capabilities and institutional stability [20, p. 427].

Given that the digital domain has evolved into a legitimate theater of war, analyzing and reconceptualizing the legal status of personal data during armed conflicts has become imperative. Because the vast majority of international humanitarian law norms emerged during the era of conventional warfare, they frequently lack effective guarantees against digital threats. Consequently, a paramount contemporary objective is to analyze existing international legal provisions aimed at protecting personal information and to develop new

ISSN 3083-7979

standards and preventive mechanisms to secure such data during modern hybrid wars.

In analyzing personal data protection within the framework of international humanitarian law, it must be reiterated that this body of law lacks specific provisions governing this domain. Instead, safeguarding the confidentiality of personal information falls under the purview of Article 27 of the 1949 Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention). This provision establishes a general obligation to respect the individual, their family rights, honor, religious convictions, customs, and traditions. The norm also mandates protection against «public curiosity,» which effectively prohibits the publication and dissemination of an individual's personal information. Furthermore, Article 33 of the same treaty merits attention, as it explicitly prohibits collective penalties, as well as any measures of intimidation or terrorism against the civilian population [18]. Evidently, while this provision does not explicitly designate personal data as a protected object, the automation of data collection and processing warrants the application of this norm by analogy. Consequently, it can be interpreted as prohibiting mass algorithmic profiling, categorization, and the collection of data intended to filter or persecute specific demographic groups within a state party to an armed conflict.

Furthermore, the provisions of the Fourth Geneva Convention concerning the operational continuity and protection of medical and hospital establishments, as well as medical personnel, deserve distinct consideration. Specifically, Article 56 of the Convention imposes such obligations on the Occupying Power. This provision can be construed as a legal guarantee for safeguarding personal medical information, given that the medical equipment, registries, and databases of military and civilian hospitals fall directly under the protective scope of this norm [14, p. 24]. Additionally, Article 52 of Additional Protocol I to the Geneva Conventions prohibits military attacks on civilian objects. Such objects may include, inter alia, the servers of state or local government authorities and private companies that store the personal information of individuals.

However, contemporary scholars remain divided on whether personal data (and information more broadly) qualify as an «object» within the meaning of international humanitarian law. A significant number of researchers concur that personal information does not constitute a civilian object from the perspective of classical international humanitarian law, given its lack of material expression and tangibility in physical space. Nevertheless, in exceptional cases, a cyberattack may be classified as a war crime, provided it inflicts tangible harm in the physical realm (for example, the deletion or alteration of medical data resulting in a patient's death; interference with automated vehicle control systems or other automated systems leading to accidents, destruction or damage to civilian infrastructure, or human casualties). Conversely, another group of scholars contends that the aforementioned approach is obsolete and inapplicable to 21st-century warfare, arguing that all norms of international law must equally apply to the digital environment. They posit that since IHL protects physical paper archives from attack, it cannot leave the exact same digitized data stored on digital media unprotected [14, p. 25]. Thus, the problem of protecting an individual's personal data during an armed conflict through the norms of international humanitarian law stems not only from the absence of specific provisions per se, but also from the divergence of opinions regarding the classification of digital data as civilian objects. This, in turn, complicates the qualification of specific actions in the digital space as international crimes and the subsequent prosecution of the perpetrators.

Regarding specialized international data protection instruments, their application is limited during armed conflicts. For instance, the provisions of the 1981 Council of Europe

ISSN 3083-7979

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (modernized) (Convention 108+) do not specifically address the application of its norms during martial law or states of emergency. This international instrument was one of the first to establish, at the regional level, the rights of the data subject, guarantees for maintaining the confidentiality of personal data, and the prohibition on the automatic processing of special categories of sensitive information. However, Article 11 of the modernized Convention 108+ of 2018, akin to the original 1981 iteration, contains provisions regarding derogations from the obligations under this treaty. Responding to a pressing social need and in accordance with the principle of proportionality, derogation from state obligations is permissible, inter alia, to protect national security and defense [10, p. 9]. Notably, the provisions of this article do not authorize a blanket derogation from all obligations under the Convention. Safeguards concerning the legitimate basis for automated data processing, its lawfulness, and the implementation of security measures against unauthorized processing, transfer, destruction, or loss of data remain in full force. Furthermore, Article 15 of Convention 108+ mandates rigorous oversight by an independent supervisory authority to ensure state compliance with the Convention's provisions [13, p. 32]. Nevertheless, the possibility of a state derogating from its obligations to ensure specific data subject rights, as established by this international treaty, necessitates deeper analysis and modernization. In the context of hybrid warfare, restricting the principle of transparent automated processing, the individual's right to access, rectify, or erase their data, and the data controller's obligation to notify the data subject of processing activities or the supervisory authority of potential data breaches, may establish a foundation for subsequent mass data collection and processing without notifying the data subjects.

Another crucial instrument that warrants mention in the context of our study is the EU General Data Protection Regulation. Specifically, Article 23 of this act contains a provision permitting restrictions on the rights and freedoms enshrined in the Regulation for the purposes of safeguarding national security and defense, provided «such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society» [12]. However, a crucial aspect must be considered: pursuant to Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of each Member State [8]. In effect, this provision exempts from the GDPR's scope all activities of a state's regular armed forces, intelligence agencies, and special services directed toward ensuring national security. Consequently, the aforementioned Article 23 and the provisions of the Regulation itself may apply during wartime almost exclusively to the relationship between state authorities and private data controllers. This creates a regulatory gap whereby the protection of individuals' personal data during wartime is left to the discretion of the states actively participating in the armed conflict. Nevertheless, it is worth noting that, unlike Convention 108+, the GDPR establishes more stringent requirements regarding the content of national legislative acts that regulate the restriction of data subject rights.

When investigating personal data protection in the context of war, it is also necessary to examine the general provisions of international human rights law. Ensuring confidentiality constitutes an integral component of the right to respect for private life, guaranteed by Article 12 of the 1948 Universal Declaration of Human Rights, Article 17 of the 1966 International Covenant on Civil and Political Rights, Article 8 of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, and other universal and regional instruments. Furthermore, the protection of personal data has been repeatedly addressed by the European Court of Human Rights. Specifically, in its

judgment in Roman Zakharov v. Russia (Application no. 47143/06), which concerned the mass interception of telephone communications by the Russian Federal Security Service without prior judicial authorization, the Court emphasized the need for clear legislative regulation of the criteria and conditions under which competent authorities may employ surveillance measures against specific categories of individuals. The ECtHR established that such legal frameworks must explicitly stipulate the grounds justifying surveillance, the categories of persons whose communications may be intercepted, the limits on the duration of the measures, the procedures for examining, using, and storing the data, the necessary precautions during data transmission, and the procedures for its destruction [4].

In its judgment in Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15), the ECtHR acknowledged the importance of mass data interception as a tool for ensuring national security and determined that, in principle, it does not contravene the provisions of the 1950 Convention. However, the Court stipulated that the interception process must be accompanied by «end-to-end safeguards.» These safeguards include, inter alia, limits on the duration of the measures, maximum data retention periods, procedures for notifying subjects upon the cessation of surveillance, and mechanisms for data subjects to challenge the respective actions [1]. The Court reached corresponding conclusions regarding adherence to the criteria of strict necessity and proportionality in the automated collection and processing of individuals' personal data for national security purposes in its rulings in Szabó and Vissy v. Hungary (Application no. 37138/14) [5] and Centrum för rättvisa v. Sweden (Application no. 35252/08) [2].

In the context of the investigated issues, the ECtHR judgment in Ukraine and the Netherlands v. Russia (Applications nos. 8019/16, 43800/14, and 28525/20) holds exceptional value. In this ruling, the Court reiterated that during armed conflicts, collecting the personal data of combatants or civilians for ostensibly legitimate purposes may conceal ulterior motives. Specifically, this includes «filtration» designed to facilitate subsequent Convention violations, such as abductions, unlawful detentions, enforced disappearances, and torture. Consequently, such activities necessitate the establishment of robust safeguards regarding search procedures, duration, storage, use, third-party access, data integrity and confidentiality preservation, and destruction protocols, alongside legislative restrictions on the conditions and scope of filtration measures [6]. Thus, although existing international human rights instruments do not directly regulate personal data protection during armed conflicts, they establish overarching guarantees regarding respect for the right to private life. Restricting this right for national security and defense purposes is permissible only given clear and sufficient grounds, strict adherence to the principle of proportionality, and the implementation of a comprehensive array of legislative safeguards ensuring the lawfulness of any interference with this human right.

Conclusions. In conclusion, the evolution of contemporary armed conflicts into hybrid warfare, coupled with rapid digitalization, has transformed personal data into a potent weapon and a strategic target for belligerent parties. Access to personal information, amplified by artificial intelligence technologies, facilitates targeted psychological influence, the dissemination of disinformation, and the identification and repression of specific demographic groups. This is starkly evidenced by the actions of the aggressor state in the temporarily occupied territories of Ukraine. However, this analysis demonstrates that the current international legal framework remains ill-equipped to address these challenges. The norms of international humanitarian law, forged during the era of conventional warfare, lack explicit guarantees for the protection of digital data. Moreover, the absence of consensus on classifying digital data as «civilian objects» significantly complicates the legal

ISSN 3083-7979

qualification of cyberattacks as war crimes. Simultaneously, specialized international privacy instruments, such as Convention 108+ and the GDPR, provide broad latitude for derogating from obligations on the grounds of national security and defense. This creates a perilous legal vacuum wherein the standards for data collection and processing during wartime are effectively left to the discretion of the states participating in the conflict. The jurisprudence of the European Court of Human Rights serves as a crucial safeguard in this context, mandating that any interference with privacy be accompanied by stringent legislative guarantees, robust oversight, and strict adherence to the principle of proportionality. Nevertheless, given the transformation of the digital domain into a fully-fledged theater of military operations, existing mechanisms are objectively insufficient to ensure comprehensive protection of the individual. Consequently, there is an urgent imperative for the international community to comprehensively reconceptualize the legal status of digital information and to develop novel, specialized standards capable of effectively safeguarding personal data amidst contemporary hybrid confrontations.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Case of Big Brother Watch and Others v. the United Kingdom : Judgement of the European Court of Human Rights. May 25, 2021. Applications nos. 58170/13, 62322/14 and 24960/15. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/fre?i=001-210077 (date of access: 25.08.2026).
2. Case of Centrum för rättvisa v. Sweden : Judgement of the European Court of Human Rights. May 25, 2021. Application no. 35252/08. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-210078 (date of access: 25.08.2026).
3. Case of Glukhin v. Russia : Judgement of the European Court of Human Rights. July 4, 2023. Application no. 11519/20. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/?i=001-225655 (date of access: 25.08.2026).
4. Case of Roman Zakharov v. Russia : Judgement of the European Court of Human Rights. December 4, 2015. Application no. 47143/06. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/fre?i=001-159324 (date of access: 25.08.2026).
5. Case of Szabó and Vissy v. Hungary : Judgement of the European Court of Human Rights. January 12, 2016. Application no. 37138/14. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/fre?i=001-160020 (date of access: 25.08.2026).
6. Case of Ukraine and the Netherlands v. Russia : Judgement of the European Court of Human Rights. July 9, 2025. Applications nos. 8019/16, 43800/14, 28525/20 and 11055/22. HUDOC – European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-244292 (date of access: 25.08.2026).
7. Cole C. B. Targeting TikTok: Adapting Distinction to the Age of Social Media. Duke University School of Law : Center on Law, Ethics and National Security, 2025. № 30. 30 p. URL: https://sites.duke.edu/lawfire/files/2025/06/Cole_Essay-6.27.25.pdf.
8. Consolidated version of the Treaty on European Union. EUR-Lex. № 12016M/TXT. 2015. URL: https://eur-lex.europa.eu/eli/treaty/teu_2016/oj/eng (date of access: 25.08.2026).
9. Hoffman F. G. Conflict in the 21st century: The rise of hybrid wars. Arlington, VA : Potomac Institute for Policy Studies, 2007. 51 p. URL: https://www.comw.org/qdr/fulltext/0712hoffman.pdf.
10. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Council of Europe. 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (date of access: 25.08.2026).
11. Pérez-Sales P. Coercion without contact: New technologies and the boundaries of torture. Torture Journal. 2026. T. 36. №. 1. P. 3-20. DOI: https://doi.org/10.7146/torture.v36i1.167351.

ISSN 3083-7979

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). № 32016R0679. April 27, 2016. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 (date of access: 25.08.2026).
13. Research Handbook on Privacy and Data Protection Law / eds. G. González, R. Van Brakel, P. De Hert. 2022. 480 p. DOI: https://doi.org/10.4337/9781786438515.
14. The Rights to Privacy and Data Protection in Times of Armed Conflict / eds. R. Buchan, A. Lubin. Tallinn : NATO CCDCOE Publications, 2022. 318 p. ISBN 978-9916-9565-7-1. URL: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1297&context=facbooks.
15. Аблазов І. В. Штучний інтелект у військовій сфері: міжнародно-правове регулювання та безпекові виклики. Академічні візії. 2025. № 46. С. 1-12. DOI: https://doi.org/10.5281/zenodo.21072124.
16. Глущенко О., Підхомний О., Ревак І. Інформаційна асиметрія інноваційного потенціалу з позицій використання штучного інтелекту в сучасних гібридних війнах. Інновації, підприємництво та економіка сучасних трансформацій у дзеркалі теорії Шумпетера : Матеріали V Міжнародної науково-практичної конференції (1-2 жовтня 2025 р.). Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2025. С. 56-58. URL: https://dspace.chnu.edu.ua/server/api/core/bitstreams/16bcac25-17d5-4785-bf06-2ad3c7f06253/content#page=56.
17. Кириченко А., Іваненко С., Ремез В. Гібридна війна як новий вимір сучасних конфліктів. Вісник Національного університету оборони України. 2025. № 86 (4). С. 85–95. DOI: https://doi.org/10.33099/2617-6858-2025-86-4-85-95.
18. Конвенція про захист цивільного населення під час війни: Женевська конвенція від 12.08.1949 р. № 995_154. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 25.08.2026).
19. Лабик А. Р. Ознаки цифрових прав людини: теоретико-правовий вимір. Вісник Маріупольського державного університету. Серія: Право. 2026. № 31. С. 214-224. DOI: https://doi.org/10.34079/2518-1319 -2026-16-31-214-224.
20. Пальчик М. Л., Шкрібляк К. П., Березделецький Ю. М. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки україни в умовах війни. Аналітично-порівняльне правознавство. 2025. №. 6. Т. 2. С. 425-434. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.69.
21. Уздєнова Ю. М. Гібридна війна: сутність, складові та ключові поняття. Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування. Київ: Київський національний університет імені Тараса Шевченка, 2024. С. 173-174. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.4/26.

REFERENCES:

1. Cole, C. B. (2025). Targeting TikTok: Adapting distinction to the age of social media (No. 30). Duke University School of Law, Center on Law, Ethics and National Security. https://sites.duke.edu/lawfire/files/2025/06/Cole_Essay-6.27.25.pdf.
2. European Union. (2015). Consolidated version of the Treaty on European Union (No. 12016M/TXT). EUR-Lex. https://eur-lex.europa.eu/eli/treaty/teu_2016/oj/eng.
3. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies. https://www.comw.org/qdr/fulltext/0712hoffman.pdf.
4. Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.
5. Pérez-Sales, P. (2026). Coercion without contact: New technologies and the boundaries of torture. Torture Journal, 36(1), 3–20. https://doi.org/10.7146/torture.v36i1.167351.

6. González, G., Van Brakel, R., & De Hert, P. (Eds.). (2022). Research Handbook on Privacy and Data Protection Law. https://doi.org/10.4337/9781786438515.
7. Buchan, R., & Lubin, A. (Eds.). (2022). The rights to privacy and data protection in times of armed conflict. NATO CCDCOE Publications. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1297&context=facbooks.
8. Ablazov, I. V. (2025). Shtuchnyi intelekt u viiskovii sferi: mizhnarodno-pravove rehuliuvannia ta bezpekovi vyklyky [Artificial intelligence in the military sphere: International legal regulation and security challenges]. Akademichni vizii, (46), 1–12. https://doi.org/10.5281/zenodo.21072124.
9. Hlushchenko, O., Pidkhomnyi, O., & Revak, I. (2025). Informatsiina asymetriia innovatsiinoho potentsialu z pozytsii vykorystannia shtuchnoho intelektu v suchasnykh hibrydnykh viinakh [Information asymmetry of innovative potential from the standpoint of using artificial intelligence in modern hybrid wars]. In Innovatsii, pidpryiemnytstvo ta ekonomika suchasnykh transformatsii u dzerkali teorii Shumpetera: Materialy V Mizhnarodnoi naukovo-praktychnoi konferentsii (pp. 56–58). Chernivetskyi natsionalnyi universytet imeni Yuriia Fedkovycha. https://dspace.chnu.edu.ua/server/api/core/bitstreams/16bcac25-17d5-4785-bf06-2ad3c7f06253/content#page=56.
10. Kyrychenko, A., Ivanenko, S., & Remez, V. (2025). Hibrydna viina yak novyi vymir suchasnykh konfliktiv [Hybrid war as a new dimension of modern conflicts]. Visnyk Natsionalnoho universytetu oborony Ukrainy, 86(4), 85–95. https://doi.org/10.33099/2617-6858-2025-86-4-85-95.
11. Konventsiia pro zakhyst tsyvilnoho naselennia pid chas viiny [Convention relative to the protection of civilian persons in time of war] (1949, August 12) (No. 995_154). https://zakon.rada.gov.ua/laws/show/995_154#Text.
12. Labyk, A. R. (2026). Oznaky tsyfrovykh prav liudyny: teoretyko-pravovyi vymir [Features of digital human rights: Theoretical and legal dimension]. Visnyk Mariupolskoho derzhavnoho universytetu. Seriia: Pravo, (31), 214–224. https://doi.org/10.34079/2518-1319-2026-16-31-214-224.
13. Palchyk, M. L., Shkribliak, K. P., & Berezdetskyi, Yu. M. (2025). Aktualni problemy zakhystu personalnykh danykh yak napriamu zabezpechennia natsionalnoi bezpeky Ukrainy v umovakh viiny [Current issues of personal data protection as a direction of ensuring national security of Ukraine in conditions of war]. Analitychno-porivnialne pravoznavstvo, (6, Vol. 2), 425–434. https://doi.org/10.24144/2788-6018.2025.06.2.69.
14. Uzdenova, Yu. M. (2024). Hibrydna viina: sutnist, skladovi ta kliuchovi poniattia [Hybrid war: Essence, components, and key concepts]. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, 35(4), 173–174. https://doi.org/10.32782/TNU-2663-6468/2024.4/26.
15. European Court of Human Rights. (2015, December 4). Case of Roman Zakharov v. Russia (Application no. 47143/06). https://hudoc.echr.coe.int/fre?i=001-159324.
16. European Court of Human Rights. (2016, January 12). Case of Szabó and Vissy v. Hungary (Application no. 37138/14). https://hudoc.echr.coe.int/fre?i=001-160020.
17. European Parliament and Council of the European Union. (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (No. 32016R0679). EUR-Lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.
18. European Court of Human Rights. (2021, May 25). Case of Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15). https://hudoc.echr.coe.int/fre?i=001-210077.

ISSN 3083-7979

19. European Court of Human Rights. (2021, May 25). Case of Centrum för rättvisa v. Sweden (Application no. 35252/08). https://hudoc.echr.coe.int/eng?i=001-210078.
20. European Court of Human Rights. (2023, July 4). Case of Glukhin v. Russia (Application no. 11519/20). https://hudoc.echr.coe.int/?i=001-225655.
21. European Court of Human Rights. (2025, July 9). Case of Ukraine and the Netherlands v. Russia (Applications nos. 8019/16, 43800/14, 28525/20 and 11055/22). https://hudoc.echr.coe.int/eng?i=001-244292.

Дата першого надходження/Date of first submission: 30.08.2026
Прийнято до друку/Accepted: 30.09.2026
Опубліковано/Published: 01.11.2026

ISSN 3083-7979